USE OF PER-FLOW MONOTONICALLY DECREASING TTLS TO PREVENT IDS CIRCUMVENTION

ABSTRACT OF THE DISCLOSURE

Systems detect maliciously formed TCP/IP retransmit packets attempting to pass through an intrusion detection system (IDS) and prevent them from reaching their destination by forcing early flow termination. As each packet arrives in the IDS, the TTL field is monotonically decreased by setting it to the smallest TTL received from the packet flow. Any packet flow that attempts to confuse the sensor with a low TTL will be starved off and will never reach the destination host. Each flow may be periodically reset to a high value or to the current packet value to allow flow recovery. In another embodiment, the TTL decrease mechanism may operate on a contingent basis, determined by the presence or absence of the flow identifier on a pre-determined list of flows that should never be restricted.